AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Western District of Washington

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Subject Premises 20 Jasmine Lane, Shelton, WA;
Subject Vehicles;
Subject Person Kyle Vance, DOB XX/XX/1995

Case No. MJ18-5269

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

The Subject Premises, Subject Vehicles and Subject Person as further described in Attachment A, which is attached hereto and incorporated herein by this reference.

located in the Western District of Washington, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, which is attached hereto and incorporated herein by this reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
Title 18, U.S.C. § 2252 (a)(2)	Receipt or Distribution of Child Pornography
Title 18, U.S.C. § 2252(a)(4)(B)	Possession of Child Pornography
Title 18, U.S.C. § 2252(b)	Enticement of a Minor
Title 18, U.S.C. § 2251	Production of Child Pornography

The application is based on these facts:

See attached Affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of ____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

SPECIAL AGENT LISSA A. EASTVOLD-WALTON, FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: 11/26/2018

Judge's signature

City and state: TACOMA, WASHINGTON

DAVID W. CHRISTEL, U.S. MAGISTRATE JUDGE
Printed name and title

2018R01387

ATTACHMENT A

Description of Property to be Searched

The address of the SUBJECT PREMISES 20 Jasmine Lane, Shelton, WA, and is more fully described as the property containing a two-story, single family home that is mostly light blue in color with white trim. The front door to the SUBJECT PREMISES is white in color. The driveway to the SUBJECT PREMISES is off of a dead end road, which appears to dead end at the SUBJECT PREMISES.

The search is to include all rooms within the SUBJECT PREMISES, all garages, parking spaces, storage units/outbuildings on the SUBJECT PREMISES and any digital device(s) found therein. However, if executing agents can reasonably determine onsite that the SUBJECT PERSON does not have access to or control over a specific area

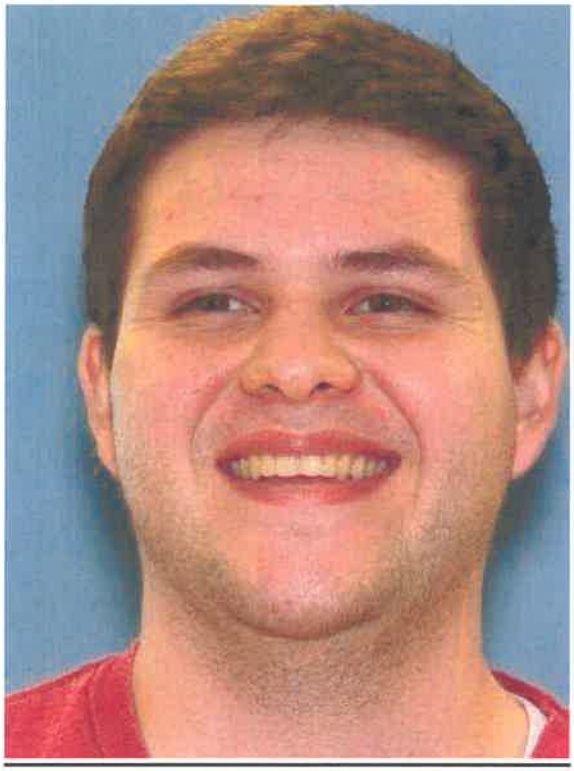
UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

within the SUBJECT PREMISES, such as the private bedroom another resident of the SUBJECT PREMISES, they will not be permitted to search that area.

SUBJECT VEHICLE 1 is a 1998 VOLKSWAGEN JETTA sedan, WA license plate AXE4194.

SUBJECT VEHICLE 2 is a 2003 Volvo sedan, WA plate BMB0759.

The SUBJECT PERSON is KYLE PAUL VANCE (DOB: XX/XX/1995), pictured below:



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT B

ITEMS TO BE SEIZED

The following records, documents, files, or materials, in whatever form, including handmade or mechanical form (such as printed, written, handwritten, or typed), photocopies or other photographic form, and electrical, electronic, and magnetic form (such as CDs, DVDs, smart cards, thumb drives, camera memory cards, electronic notebooks, or any other storage medium), that constitute evidence, instrumentalities, or fruits of violations of 18 U.S.C. § 2422(b) (Enticement of a Minor), 18 U.S.C. § 2251 (Production of Child Pornography), 18 U.S.C. § 2252(a)(2) (Receipt or Distribution of Child Pornography), and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography), which may be found at the SUBJECT PREMISES, in the SUBJECT VEHICLE, or on the SUBJECT PERSON:

1. Any visual depiction of minor(s) engaged in sexually explicit conduct and child erotica, in any format or media and any items depicted in those visual depictions that may help to identify the person depicted or the creator of the depictions;

2. Evidence of the installation and use of P2P software, and any associated logs, saved user names and passwords, shared files, and browsing history;

3. Letters, e-mail, text messages, and other correspondence identifying persons transmitting child pornography, or evidencing the transmission of child pornography, through interstate or foreign commerce, including by mail or by computer;

4. All invoices, purchase agreements, catalogs, canceled checks, money order receipts, credit card statements or other documents pertaining to the transportation or purchasing of images of minors engaged in sexually explicit conduct;

5. Any and all address books, names, lists of names, telephone numbers, and addresses of individuals engaged in the transfer, exchange, or sale of child pornography;

6. Any non-digital recording devices and non-digital media capable of storing images and videos.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

7. Digital devices and/or their components, which include, but are not limited to:

a. Any digital devices and storage device capable of being used to commit, further, or store evidence of the offense listed above;

b. Any digital devices used to facilitate the transmission, creation, display, encoding or storage of data, including word processing equipment, modems, docking stations, monitors, cameras, printers, encryption devices, and optical scanners;

c. Any magnetic, electronic, or optical storage device capable of storing data, such as disks, tapes, CD-ROMs, CD-Rs, CD-RWs, DVDs, printer or memory buffers, smart cards, PC cards, memory sticks, flashdrives, USB/thumb drives, camera memory cards, media cards, electronic notebooks, and personal digital assistants;

d. Any documentation, operating logs and reference manuals regarding the operation of the digital device or software;

e. Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices, or data to be searched;

f. Any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the computer equipment, storage devices or data; and

g. Any passwords, password files, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data;

8. Evidence of who used, owned or controlled any seized digital device(s) at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, saved user names and passwords, documents, and browsing history;

9. Evidence of malware that would allow others to control any seized digital device(s) such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malware; as well as evidence of the lack of such malware;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

10. Evidence of the attachment to the digital device(s) of other storage devices or similar containers for electronic evidence;

11. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from a digital device;

12. Evidence of times the digital device(s) was used;

13. Any other ESI from the digital device(s) necessary to understand how the digital device was used, the purpose of its use, who used it, and when.

14. Records and things evidencing the use of the IP address 73.109.71.123 (the SUBJECT IP ADDRESS) including:

a. Routers, modems, and network equipment used to connect computers to the Internet;

b. Records of Internet Protocol (IP) addresses used;

c. Records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

The seizure of digital devices and/or their components as set forth herein is specifically authorized by this search warrant, not only to the extent that such digital devices constitute instrumentalities of the criminal activity described above, but also for the purpose of the conducting off-site examinations of their contents for evidence, instrumentalities, or fruits of the aforementioned crimes.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

AFFIDAVIT

STATE OF WASHINGTON)
) ss
COUNTY OF PIERCE)

I, Lissa Eastvold-Walton, being duly sworn on oath, depose and state:

I. INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent ("SA") with the Federal Bureau of Investigation ("FBI"). I have been employed as an FBI SA since June 2014, and am currently assigned to the Seattle Division's Tacoma Resident Agency. Prior to becoming a SA, I was employed as a licensed professional counselor and attended graduate school to earn a doctoral degree in rehabilitation psychology. While employed by the FBI, I have investigated a broad variety of federal criminal violations, including mail fraud, wire fraud, public corruption, health care fraud, physical and sexual assault, and child pornography. I have gained experience through training at the FBI Academy and everyday work relating to conducting these types of investigations. I am currently authorized to investigate and enforce violations of federal criminal statutes, including those found in Title 18 and 21 of the United States Code. Furthermore, as an "investigative or law enforcement officer" of the United States, I am empowered by law to conduct investigations of, and to make arrests for, criminal violations relating to child exploitation and child pornography including violations of Title 18, United States Code, Sections 2251 and 2252.

2. I am submitting this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the residence located at 20 Jasmine Lane, Shelton, Washington 98584 (hereinafter the "SUBJECT PREMISES") more fully described in Attachment A, the person of KYLE PAUL VANCE (the "SUBJECT PERSON"), a 1998 VOLSWAGEN JETTA sedan, license plate AXE4194,

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

("SUBJECT VEHICLE 1"), and a 2003 Volvo sedan, WA plate BMB0759 ("SUBJECT VEHICLE 2") for the things specified in Attachment B to this Affidavit, for the reasons set forth below. I also seek authority to examine digital devices or other electronic storage media. The property and person to be searched is as follows. The warrant would authorize a search of the SUBJECT PREMISES, the SUBJECT PERSON, and the SUBJECT VEHICLES, as well as the seizure and forensic examination of digital devices found therein, for the purpose of identifying electronically stored data as particularly described in Attachment B, for evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2422(b) (Enticement of a Minor), 18 U.S.C. § 2251 (Production of Child Pornography), 18 U.S.C. § 2252(a)(2) (Receipt or Distribution of Child Pornography), and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography).

3. The facts set forth in this Affidavit are based on my own personal knowledge; knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers; review of documents and records related to this investigation; communications with others who have personal knowledge of the events and circumstances described herein; and information gained through my training and experience.

4. Because this affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact that I or others have learned during the course of this investigation. I have set forth only the facts that I believe are relevant to the determination of probable cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2422(b) (Enticement of a Minor), 18 U.S.C. § 2251 (Production of Child Pornography), 18 U.S.C. § 2252(a)(2) (Receipt or Distribution of Child Pornography), and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography) will be found at the SUBJECT PREMISES, in the SUBJECT VEHICLES, and on the SUBJECT PERSON.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

II. STATEMENT OF PROBABLE CAUSE

5. On or about January 12, 2018, J.P. came to the Gravette Police Department in Arkansas to report his nine-year-old daughter (MV) sent explicit photographs to an individual later identified as KYLE PAUL VANCE using Facebook Messenger.

6. A forensic interview was set up for MV that same day. During the interview, MV stated she first met VANCE while playing a game on her tablet called "Party in my Dorm." MV stated she sent a request to VANCE on the game. MV stated VANCE accepted the request and they started talking. MV said VANCE then asked her to send him pictures. MV stated she told VANCE she could not send pictures through the game, and VANCE told MV to add him on Facebook Messenger. MV did so, and VANCE again asked her to send him photos.

7. According to MV, she sent VANCE an old picture of her sister as a fifteen-year-old. MV said VANCE then asked her to send him photos of her private areas. MV said she initially refused but that she eventually gave in to VANCE's request because he continued to ask for them. MV stated she went behind her bed and took photographs of herself and sent them to VANCE. MV stated she sent a picture of her genitals and a picture of her breasts to VANCE.

8. MV said that after she sent the photographs to VANCE the two video chatted on Facebook Messenger, and VANCE appeared to be holding a microphone in his hand. MV stated she discontinued the video chat and then sent a picture of her buttocks to VANCE. She said VANCE then sent her a picture of his "peepee."

9. MV said that she told VANCE she was fifteen because she thought VANCE would tell her to get off the game if he knew she were only nine.

10. On February 21, 2018, Special Agent Reuben Gay met with MV's father, who gave consent for the FBI to assume MV's identity on Facebook. On February 26, 2018, SA Gay accessed MV's Facebook account and saw the following conversation with VANCE that took place on December 22, 2017:

VANCE: I want to see you now

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

MV: (MV sent two pictures of what appears to be her older sister)

VANCE: Why don't you just take a selfie (VANCE takes selfie of his face and sends to MV)

MV: Dude as I told you I have no clothes on and I'm really lazy also I look horrible.

VANCE: You can cover up and I'm sure you don't look that bad

MV: (sends a picture of her partially concealed face)

VANCE: I still can't see much

MV: (sends another picture showing more of her face)

VANCE: you look super cute

MV: I'm going back to the game

VANCE: but you are nice to look at

MV: thanks

VANCE: you are adorable

MV: thanks

VANCE: You're welcome sweetie

(Emoji's exchanged)

MV: I'm eating another peach

VANCE: Do you have a nice peach? (Emoji's followed)

MV: Yes (Followed by emoji's)

VANCE: Lemme see I like peaches

MV: (sends a smile emoji), I'm not sure my mom would approve

VANCE: now you are teasing me, saying you have a nice thing and not sharing

MV: OK but only if you don't show anyone

VANCE: of course not, thanks sweetie

VANCE: are you still there

MV: it's really hard to take a pict of just my peaches

VANCE: you can show more if you want

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

MV: ok

VANCE: you are so nice and sweet

MV: I will just take a picture of something else.

VANCE: ok

MV: (sends a close up picture of what appear to be the genitals of a young girl)

VANCE: mmm can I see the rest of you

VANCE: Wow you are sexy

VANCE: You make me s hard

VANCE: And now you are going to tease me, come on babe.

MV: Well what else do you want to see, cause I think I want to see something…

VANCE: (sends eggplant emoji), if you want to do a video chat I will show you.

MV: A. is in the room over and my parents are in the room right beside me.

VANCE: I'm not going to make any noise

MV: My parents might hear me talking so send a Pict.

VANCE: we can do no talking and I will stroke my dick for you

MV: ok fine ofnly for 3 min

(They video chat)

VANCE: Let me see you now

MV: I won't be able to video chat tho

VANCE: ok fine

MV: (sends another photograph of what appear to be a young girl's genitals)

I have small boobs and don't want to show them

VANCE: awe come on

MV: they are extremely small

VANCE: its's fine

MV: (sends picture of a young girl's chest)

(MV then asks VANCE to send a picture of his penis using an eggplant emoji)

VANCE: why you want a pict so bad?

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

MV: you don't have to

VANCE: I will only show with video chat so others don't see

MV: we can't talk anymore my mom checks my tablet daily, bye

VANCE: ok

11. The pictures sent by MV showing her face were partially obscured. In the photos, MV is covering the lower half of her face with what appears to be a book, exposing only her nose, eyes and forehead. However, MV's publicly visible Facebook profile photo contained a clear picture of her face. I have examined this photo, and it clearly depicts a child under the age of twelve.

12. On or about August 23, 2018, SA Gay obtained a search warrant identifying information and content for the Facebook profile belonging to VANCE.

13. On or about September 5, 2018, Facebook returned subscriber information and content for VANCE's account. According to Facebook, VANCE's account was created on January 22, 2009, with email address kylevance@live.com. VANCE listed a residence in Rexburg, Idaho.

14. SA Gay reviewed the Facebook search warrant return, which included the Facebook messenger communications between VANCE and MV, which took place December 22, 2017. These messages were the same messages seen in MV's Facebook account described above. SA Gay noted the communications were sexually explicit, and he saw three sexually explicit files exchanged between MV and VANCE. SA Gay also saw that VANCE described MV as "adorable, sweetie, and super cute." In addition to the conversation outlined above, VANCE repeatedly asked MV to send explicit photographs stating, "now you are just teasing me", "mmmmm can I see the rest of you", " wow you're sexy", "you make me so hard".

15. SA Gay also found messages between VANCE and another individual ("BATTLE") via Facebook Messenger, which further demonstrate VANCE's apparent sexual interest in minors. BATTLE sends VANCE a photograph of a girl who she refers

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

to as her "cousin" and states that she is "shes 5." The following excerpts are from their conversation:

VANCE: You didn't answer my question

BATTLE: what question

VANCE: Do you have a sexy ass?

BATTLE: Oh idk

BATTLE: im fat

BATTLE: soooo

VANCE: soooo that's a yes?

BATTLE: ?

BATTLE: sorry still tired so I don't understand

VANCE: that you got a sexy ass

BATTLE: oh sure

BATTLE: that's what my little cousin tell me lol

VANCE: Well do I get to see it to tell you as well?

BATTLE: nawww

VANCE: Come on I know you want to

BATTLE: want to what

VANCE: show me dat ass

BATTLE: whyy

VANCE: Cuz I asked

BATTLE: but you first

VANCE: Maybe later

BATTLE: I wanna be someones princess

VANCE: You can be mine

BATTLE: but you're far away and I don't think you can handle me

BATTLE: I need someone special

VANCE: Well then in that case I guess we are done talking

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

BATTLE: Fight me

BATTLE: im sooo single

BATTLE: im bored

VANCE: Lol what's up

BATTLE: i need someone to talk to

VANCE: ok well I'm here

VANCE: And if I send you a booty pic do I still get to see yours

BATTLE: Kids lool

VANCE: kids??

BATTLE: call and youll see

VANCE: Nah

BATTLE: why not

VANCE: I don't want to deal with a bunch of screaming kids

BATTLE: they stopped screaming

VANCE: Still don't want that

VANCE: And you won't even show me if you got a nice ass

BATTLE: well you wont call to see soooo lol

VANCE: Why can't you just take a pic?

BATTLE: fine

VANCE: Woohoo

BATTLE: (Sent a picture of a young girl, wearing short pink shorts, on her hands and knees with her buttocks facing the camera)

BATTLE: princess of my 🖤 sent a photo.

VANCE: Ooooh😍

VANCE: That's a nice ass😉

VANCE: Do you like it being grabbed?

BATTLE: cousin said thank you

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

VANCE: Lol you're ridiculous □ 😂

BATTLE: 😂😂ikr

VANCE: Well maybe I should talk with her instead ☺😂

BATTLE: shes 5 😂😂😂😂😂😂

VANCE: And she's nicer then you😂😂

VANCE: (Sent a photo of his face)

BATTLE: she said she wanna go out with you😂☺

VANCE: Well let me talk with her then☺😂😂😂

BATTLE: you can call😂😂😂😂

VANCE: I can't call right now I might call tomorrow

VANCE: But let's see her face if she wants to go out with me

VANCE: 😂😂

BATTLE: (Sent a photo of two young girls with one girl appeared to blow a kiss at the camera)

BATTLE: 😂😂😂

VANCE: She blowing the kiss?

BATTLE: yea

VANCE: She's a cutie☺

VANCE: Maybe I should go out with her☺

BATTLE: (Sent a picture with the her and the two minor girls)

VANCE: That you on the end?

BATTLE: yea

VANCE: Dang you both cuties❤

VANCE: Hmm which one of you wants to go out with me.more?

BATTLE: the baby thicc too😂

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

VANCE: You trying to get me to do all of you□😂😂😂😂

BATTLE: maybeeee😉😂😂😂😂

VANCE: You want a foursome?

BATTLE: the dog thicc too😂🙂

VANCE: I'd consider a threesome with you and the one that blew me a kiss but I don't think I'd do the baby😂

BATTLE: awe😂

VANCE: So can you and the cutie with the nice booty take a pic side by side😂

VANCE: Are you busy?

VANCE: I thought you wanted to talk?

BATTLE: (Sent a picture with her and the five year old side by side. Battle's back was facing the camera. Battle is wearing underwear and a bra and the five year old has her underwear rolled up between her buttocks and was on all fours with her back facing the camera)

VANCE: Oh dang can I do both of you😍😍

VANCE: Let's see the fronts too😉

BATTLE: wym the front😂

VANCE: I saw your ass so let's see your tits😂

VANCE: And dang you're both hella sexy ❤

VANCE: (Sent a picture with no shirt on)

BATTLE: she said thank you soooo much😯

BATTLE: and im wearing a bra

VANCE: Aww she's a cutie 😯

VANCE: Soooo take it off😂😂

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

BATTLE: (Sent a photograph sitting next to the five year old girl. Battle was topless and the five year old had her shirt pulled back behind her head revealing her bare chest)

VANCE: Dang y'all are hot af😈🍆

BATTLE: thanks papi☺

VANCE: Mmmm can you have her suck your tits 🍆□

BATTLE: (Sent a photograph of the five year old girl sucking on Battle's bare breast)

VANCE: Hey I have to go somewhere in a couple minutes but when I get back I will call you

VANCE: Mmmmm baby you're so naughty 😍😍😍

VANCE: Can you do a video of you fingering each other😈😈🍆🍆🍆

BATTLE: that felt kinda weird😂😂😂

VANCE: You're amazing baby all of you😍😍😍❤❤❤❤❤😵😵😵😵

BATTLE: but shes sooo young😂😂😂

VANCE: She seems to like it tho☺

VANCE: If she doesn't like it then you don't need to

BATTLE: she thinks its weird too

VANCE: Ok then can you do a video of you dancing naked

VANCE: ??

VANCE: Or is that wierd as well?

BATTLE: she said thats weird

VANCE: To dance?

VANCE: Alright then you come up with something and surprise me❤😵

BATTLE: the naked part

VANCE: Oh gotcha

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

VANCE: Maybe just topless?

VANCE: Ok I gtg now I'll be back later and I'll call you❤❤☺

BATTLE: she said that sounds really weird

VANCE: Ok I'll talk later

16. Based on information received during the investigation, I believe that the SUBJECT PERSON is residing at the SUBJECT PREMISES with other family members, to include his mother, brothers, and grandparents. Results of a fee-for-service database search and information received from the Department of Licensing and the Department of Corrections reveal that the SUBJECT PERSON is residing at the SUBJECT PREMISES. Information received from the Department of Licensing revealed that the SUBJECT PERSON is the registered owner of a 1998 VOLKSWAGEN JETTA sedan, Washington license plate AXE4194 (SUBJECT VEHICLE 1) and a 2003 Volvo sedan, WA plate BMB0759 ("SUBJECT VEHICLE 2") . The primary address listed on the vehicle registration is the SUBJECT PREMISES. The SUBJECT PERSON's grandfather, who resides at the SUBJECT PREMISES was sentenced to prison time following the conviction of child molestation in 1992. One of the SUBJECT PERSON's brothers is a registered sexual offender and on Department of Corrections supervision until 2027.

III. PRIOR EFFORTS TO OBTAIN EVIDENCE

17. Any other means of obtaining the necessary evidence to prove the elements of computer/Internet-related crimes, for example, a consent search, could result in an unacceptable risk of the loss/destruction of the evidence sought. If agents pursued a consent-based interview with the SUBJECT PERSON, or any other unknown resident(s) or occupant(s) of the SUBJECT PREMISES, they could rightfully refuse to give consent and the user who distributed child pornography files as outlined above could arrange for destruction of all evidence of the crime before agents could return with a search warrant. Based on my knowledge, training and experience, the only effective means of collecting

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

and preserving the required evidence in this case is through a search warrant. Based on my knowledge, no prior search warrant has been obtained to search the SUBJECT PREMISES or the SUBJECT PERSON.

IV. TECHNICAL BACKGROUND

18. Based on my training and experience, when an individual communicates through the Internet, the individual leaves an IP address which identifies the individual user by account and ISP (as described above). When an individual is using the Internet, the individual's IP address is visible to administrators of websites they visit. Further, the individual's IP address is broadcast during most Internet file and information exchanges that occur.

19. As noted above, this investigation involves the use of Facebook messenger service. Facebook Inc., a social networking company headquartered in Menlo Park, California, has a feature which allows users to communicate through Facebook messenger. Facebook messenger allows individuals to communicate with other users by sending texts, pictures, and videos. Users can send and receive messages, images, videos, and other content to other users.

20. Based on my training and experience, I know that most ISPs provide only one IP address for each residential subscription. I also know that individuals often use multiple digital devices within their home to access the Internet, including desktop and laptop computers, tablets, and mobile phones. A device called a router is used to connect multiple digital devices to the Internet via the public IP address assigned (to the subscriber) by the ISP. A wireless router performs the functions of a router but also includes the functions of a wireless access point, allowing (wireless equipped) digital devices to connect to the Internet via radio waves, not cables. Based on my training and experience, today many residential Internet customers use a wireless router to create a computer network within their homes where users can simultaneously access the Internet (with the same public IP address) with multiple digital devices.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

21. Based on my training and experience and information provided to me by computer forensic agents, I know that data can quickly and easily be transferred from one digital device to another digital device. Data can be transferred from computers or other digital devices to internal and/or external hard drives, tablets, mobile phones, and other mobile devices via a USB cable or other wired connection. Data can also be transferred between computers and digital devices by copying data to small, portable data storage devices including USB (often referred to as "thumb") drives, memory cards (Compact Flash, SD, microSD, etc.) and memory card readers, and optical discs (CDs/DVDs).

22. As outlined above, residential Internet users can simultaneously access the Internet in their homes with multiple digital devices. Also explained above is how data can quickly and easily be transferred from one digital device to another through the use of wired connections (hard drives, tablets, mobile phones, etc.) and portable storage devices (USB drives, memory cards, optical discs). Therefore, a user could access the Internet using their assigned public IP address, receive, transfer or download data, and then transfer that data to other digital devices, which may or may not have been connected to the Internet during the date and time of the specified transaction.

23. Based on my training and experience, I have learned that the computer's ability to store images and videos in digital form makes the computer itself an ideal repository for child pornography. The size of hard drives used in computers (and other digital devices) has grown tremendously within the last several years. Hard drives with the capacity of four (4) terabytes (TB) are not uncommon. These drives can store thousands of images and videos at very high resolution.

24. Based on my training and experience, and information provided to me by other law enforcement officers, I know that people tend to use the same user names across multiple accounts and email services.

25. Based on my training and experience, collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by companies such as Google, Yahoo, Apple, and Dropbox, among

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

others. The online services allow a user to set up an account with a remote computing service that provides email services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer in most cases.

26. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an email as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" and history files of the browser application used. A forensic examiner often can recover evidence suggesting whether a computer contains wireless software, and when certain files under investigation were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data.

27. Based on my training and experience, I have learned that producers of child pornography can produce image and video digital files from the average digital camera, mobile phone, or tablet. These files can then be easily transferred from the mobile device to a computer or other digital device, using the various methods described above. The digital files can then be stored, manipulated, transferred, or printed directly from a computer or other digital device. Digital files can also be edited in ways similar to those by which a photograph may be altered; they can be lightened, darkened, cropped, or otherwise manipulated. As a result of this technology, it is relatively inexpensive and technically easy to produce, store, and distribute child pornography. In addition, there is

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

an added benefit to the child pornographer in that this method of production is a difficult trail for law enforcement to follow.

28. As part of my training and experience, I have become familiar with the structure of the Internet, and I know that connections between computers on the Internet routinely cross state and international borders, even when the computers communicating with each other are in the same state. Individuals and entities use the Internet to gain access to a wide variety of information; to send information to, and receive information from, other individuals; to conduct commercial transactions; and to communicate via email.

29. Based on my training and experience, I know that cellular mobile phones (often referred to as "smart phones") have the capability to access the Internet and store information, such as images and videos. As a result, an individual using a smart phone can send, receive, and store files, including child pornography, without accessing a personal computer or laptop. An individual using a smart phone can also easily connect the device to a computer or other digital device, via a USB or similar cable, and transfer data files from one digital device to another. Moreover, many media storage devices, including smartphones and thumb drives, can easily be concealed and carried on an individual's person and smartphones and/or mobile phones are also often carried on an individual's person.

30. As set forth herein and in Attachment B to this Affidavit, I seek permission to search for and seize evidence, fruits, and instrumentalities of the above-referenced crimes that might be found at the SUBJECT PREMISES, in the SUBJECT VEHICLES, or on the SUBJECT PERSON, in whatever form they are found. It has been my experience that individuals involved in child pornography often prefer to store images of child pornography in electronic form. The ability to store images of child pornography in electronic form makes digital devices, examples of which are enumerated in Attachment B to this Affidavit, an ideal repository for child pornography because the images can be

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

easily sent or received over the Internet. As a result, one form in which these items may be found is as electronic evidence stored on a digital device.

31. Based upon my knowledge, experience, and training in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know that there are certain characteristics common to individuals who have a sexualized interest in children and depictions of children:

a. They may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

b. They may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides, and/or drawings or other visual media. Such individuals often times use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts. These individuals may keep records, to include names, contact information, and/or dates of these interactions, of the children they have attempted to seduce, arouse, or with whom they have engaged in the desired sexual acts.

c. They often maintain any "hard copies" of child pornographic material that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. These individuals typically retain these "hard copies" of child pornographic material for many years, as they are highly valued.

d. Likewise, they often maintain their child pornography collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections are often maintained for several

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

years and are kept close by, often at the individual's residence or some otherwise easily accessible location, to enable the owner to view the collection, which is valued highly.

e. They also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f. They generally prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

g. E-mail itself provides a convenient means by which individuals can access a collection of child pornography from any computer, at any location with Internet access. Such individuals therefore do not need to physically carry their collections with them but rather can access them electronically. Furthermore, these collections can be stored on email "cloud" servers, which allow users to store a large amount of material at no cost, without leaving any physical evidence on the users' computer(s).

32. In addition to offenders who collect and store child pornography, law enforcement has encountered offenders who obtain child pornography from the internet, view the contents and subsequently delete the contraband, often after engaging in self-gratification. In light of technological advancements, increasing Internet speeds and worldwide availability of child sexual exploitative material, this phenomenon offers the offender a sense of decreasing risk of being identified and/or apprehended with quantities of contraband. This type of consumer is commonly referred to as a 'seek and delete' offender, knowing that the same or different contraband satisfying their interests remain easily discoverable and accessible online for future viewing and self-gratification. I know that, regardless of whether a person discards or collects child pornography he/she accesses for purposes of viewing and sexual gratification, evidence of such activity is

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

likely to be found on computers and related digital devices, including storage media, used by the person. This evidence may include the files themselves, logs of account access events, contact lists of others engaged in trafficking of child pornography, backup files, and other electronic artifacts that may be forensically recoverable.

33. Given the above-stated facts, and based on my knowledge, training and experience, along with my discussions with other law enforcement officers who investigate child exploitation crimes, I believe that the SUBJECT PERSON likely has a sexualized interest in children and depictions of children and that evidence of child pornography is likely to be found on digital media devices, including mobile and/or portable digital devices found at the SUBJECT PREMISES, in the SUBJECT VEHICLES, or on the SUBJECT PERSON.

34. Based on my training and experience, and that of computer forensic agents that I work and collaborate with on a daily basis, I know that every type and kind of information, data, record, sound or image can exist and be present as electronically stored information on any of a variety of computers, computer systems, digital devices, and other electronic storage media. I also know that electronic evidence can be moved easily from one digital device to another. As a result, I believe that electronic evidence may be stored on any digital device present at the SUBJECT PREMISES, in the SUBJECT VEHICLES, or on the SUBJECT PERSON.

35. Based on my training and experience, and my consultation with computer forensic agents who are familiar with searches of computers, I know that in some cases the items set forth in Attachment B may take the form of files, documents, and other data that is user-generated and found on a digital device. In other cases, these items may take the form of other types of data - including in some cases data generated automatically by the devices themselves.

36. Based on my training and experience, and my consultation with computer forensic agents who are familiar with searches of computers, I believe that if digital devices are found in the SUBJECT PREMISES, in the SUBJECT VEHICLES, or on the

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

SUBJECT PERSON, there is probable cause to believe that the items set forth in Attachment B will be stored in those digital devices for a number of reasons, including but not limited to the following:

a. Once created, electronically stored information (ESI) can be stored for years in very little space and at little or no cost. A great deal of ESI is created, and stored, moreover, even without a conscious act on the part of the device operator. For example, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache," without the knowledge of the device user. The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages or if a user takes affirmative steps to delete them. This ESI may include relevant and significant evidence regarding criminal activities, but also, and just as importantly, may include evidence of the identity of the device user, and when and how the device was used. Most often, some affirmative action is necessary to delete ESI. And even when such action has been deliberately taken, ESI can often be recovered, months or even years later, using forensic tools.

b. Wholly apart from data created directly (or indirectly) by user-generated files, digital devices - in particular, a computer's internal hard drive - contain electronic evidence of how a digital device has been used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating systems or application operations, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible for a user to use such specialized software to delete this type of information - and, the use of such special software may itself result in ESI that is relevant to the criminal investigation. In particular, to properly retrieve and analyze electronically stored (computer) data, and to ensure accuracy and completeness of such data and to prevent loss of the data either from accidental or programmed destruction, it is necessary

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

to conduct a forensic examination of the computers. To effect such accuracy and completeness, it may also be necessary to analyze not only data storage devices, but also peripheral devices which may be interdependent, the software to operate them, and related instruction manuals containing directions concerning operation of the computer and software.

V. SEARCH AND/OR SEIZURE OF DIGITAL DEVICES

37. In addition, based on my training and experience and that of computer forensic agents that I work and collaborate with on a daily basis, I know that in most cases it is impossible to successfully conduct a complete, accurate, and reliable search for electronic evidence stored on a digital device during the physical search of a search site for a number of reasons, including but not limited to the following:

a. Technical Requirements: Searching digital devices for criminal evidence is a highly technical process requiring specific expertise and a properly controlled environment. The vast array of digital hardware and software available requires even digital experts to specialize in particular systems and applications, so it is difficult to know before a search which expert is qualified to analyze the particular system(s) and electronic evidence found at a search site. As a result, it is not always possible to bring to the search site all of the necessary personnel, technical manuals, and specialized equipment to conduct a thorough search of every possible digital device/system present. In addition, electronic evidence search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since ESI is extremely vulnerable to inadvertent or intentional modification or destruction (both from external sources and from destructive code embedded in the system such as a "booby trap"), a controlled environment is often essential to ensure its complete and accurate analysis.

b. Volume of Evidence: The volume of data stored on many digital devices is typically so large that it is impossible to search for criminal evidence in a

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

reasonable period of time during the execution of the physical search of a search site. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Computer hard drives are now being sold for personal computers capable of storing up to four terabytes (4,000 gigabytes of data.) Additionally, this data may be stored in a variety of formats or may be encrypted (several new commercially available operating systems provide for automatic encryption of data upon shutdown of the computer).

c. Search Techniques: Searching the ESI for the items described in Attachment B may require a range of data analysis techniques. In some cases, it is possible for agents and analysts to conduct carefully targeted searches that can locate evidence without requiring a time-consuming manual search through unrelated materials that may be commingled with criminal evidence. In other cases, however, such techniques may not yield the evidence described in the warrant, and law enforcement personnel with appropriate expertise may need to conduct more extensive searches, such as scanning areas of the disk not allocated to listed files, or peruse every file briefly to determine whether it falls within the scope of the warrant.

38. In this particular case, and in order to protect the third party privacy of innocent individuals residing in the residence, the following are search techniques that will be applied:

i. Device use and ownership will be determined through interviews, if possible, and through the identification of user account(s), associated account names, and logons associated with the device. Determination of whether a password is used to lock a user's profile on the device(s) will assist in knowing who had access to the device or whether the password prevented access.

ii. Use of hash value library searches.

iii. Use of keyword searches, i.e., utilizing key words that are known to be associated with the sharing of child pornography.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

iv. Identification of non-default programs that are commonly known to be used for the exchange and viewing of child pornography, such as, eMule, uTorrent, BitTorrent, Ares, Shareaza, Gnutella, etc.

v. Looking for file names indicative of child pornography, such as, PTHC, PTSC, Lolita, 3yo, etc. and file names identified during the undercover download of child pornography.

vi. Viewing of image files and video files.

vii. As indicated above, the search will be limited to evidence of child pornography and will not include looking for personal documents and files that are unrelated to the crime.

39. These search techniques may not all be required or used in a particular order for the identification of digital devices containing items set forth in Attachment B to this Affidavit. However, these search techniques will be used systematically in an effort to protect the privacy of third parties. Use of these tools will allow for the quick identification of items authorized to be seized pursuant to Attachment B to this Affidavit, and will also assist in the early exclusion of digital devices and/or files which do not fall within the scope of items authorized to be seized pursuant to Attachment B to this Affidavit.

40. In accordance with the information in this Affidavit, law enforcement personnel will execute the search of digital devices seized pursuant to this warrant as follows:

a. Upon securing the search site, the search team will conduct an initial review of any digital devices/systems to determine whether the ESI contained therein can be searched and/or duplicated on site in a reasonable amount of time and without jeopardizing the ability to accurately preserve the data.

b. If, based on their training and experience, and the resources available to them at the search site, the search team determines it is not practical to make an on-site search, or to make an on-site copy of the ESI within a reasonable amount of

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

time and without jeopardizing the ability to accurately preserve the data, then the digital devices will be seized and transported to an appropriate law enforcement laboratory for review and to be forensically copied ("imaged"), as appropriate.

c. In order to examine the ESI in a forensically sound manner, law enforcement personnel with appropriate expertise will produce a complete forensic image, if possible and appropriate, of any digital device that may contain data or items that fall within the scope of Attachment B of this Affidavit. In addition, appropriately trained personnel may search for and attempt to recover deleted, hidden, or encrypted data to determine whether the data fall within the list of items to be seized pursuant to the warrant. In order to search fully for the items identified in the warrant, law enforcement personnel, which may include investigative agents, may then examine all of the data contained in the forensic image/s and/or on the digital devices to view their precise contents and determine whether the data fall within the list of items to be seized pursuant to the warrant.

d. The search techniques that will be used will be only those methodologies, techniques and protocols as may reasonably be expected to find, identify, segregate and/or duplicate the items authorized to be seized pursuant to Attachment B to this Affidavit.

e. If, after conducting its examination, law enforcement personnel determine that any digital device is an instrumentality of the criminal offenses referenced above, the government may retain that device during the pendency of the case as necessary to, among other things, preserve the instrumentality evidence for trial, ensure the chain of custody, and litigate the issue of forfeiture.

41. Because multiple individuals may reside at the SUBJECT PREMISES, executing agents will take reasonable steps to protect the privacy of third-parties who are not suspected of a crime. Executing agents will therefore attempt to determine onsite what areas within the SUBJECT PREMISES the SUBJECT PERSON has access to and/or control over. If executing agents reasonably determine that the SUBJECT

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

PERSON does not have access to or control over a specific area, such as the private bedroom another resident at the SUBJECT PREMISES, they will not search that area.

42. In order to search for ESI that falls within the list of items to be seized pursuant to Attachment B to this Affidavit, law enforcement personnel will seize and search the following items (heretofore and hereinafter referred to as "digital devices"), subject to the procedures set forth above:

a. Any digital device capable of being used to commit, further, or store evidence of the offense(s) listed above;

b. Any digital device used to facilitate the transmission, creation, display, encoding, or storage of data, including word processing equipment, modems, docking stations, monitors, printers, cameras, encryption devices, and optical scanners;

c. Any magnetic, electronic, or optical storage device capable of storing data, such as disks, tapes, CD-ROMs, CD-Rs, CD-RWs, DVDs, printer or memory buffers, smart cards, PC cards, memory sticks, flash drives, thumb drives, camera memory cards, media cards, electronic notebooks, and personal digital assistants;

d. Any documentation, operating logs and reference manuals regarding the operation of the digital device, or software;

e. Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the device hardware, or ESI to be searched;

f. Any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the digital device, or ESI; and

g. Any passwords, password files, test keys, encryption codes or other information necessary to access the digital device or ESI.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

VI. CONCLUSION

43. Based on the foregoing, I believe there is probable cause that evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2422(b) (Enticement of a Minor), 18 U.S.C. § 2251 (Production of Child Pornography), 18 U.S.C. § 2252(a)(2) (Receipt or Distribution of Child Pornography), and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography) are located at the SUBJECT PREMISES, in the SUBJECT VEHICLES, or on the SUBJECT PERSON as more fully described in Attachment A to this Affidavit, as well as on and in any digital devices found therein. I therefore request that the court issue a warrant authorizing a search of the location, vehicles, and person specified in Attachment A for the items more fully described in Attachment B.

Lissa A. Eastvold-Walton, Affiant
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me this 26th day of November, 2018.

DAVID W. CHRISTEL
United States Magistrate Judge

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT A

Description of Property to be Searched

The address of the SUBJECT PREMISES 20 Jasmine Lane, Shelton, WA, and is more fully described as the property containing a two-story, single family home that is mostly light blue in color with white trim. The front door to the SUBJECT PREMISES is white in color. The driveway to the SUBJECT PREMISES is off of a dead end road, which appears to dead end at the SUBJECT PREMISES.

The search is to include all rooms within the SUBJECT PREMISES, all garages, parking spaces, storage units/outbuildings on the SUBJECT PREMISES and any digital device(s) found therein. However, if executing agents can reasonably determine onsite that the SUBJECT PERSON does not have access to or control over a specific area

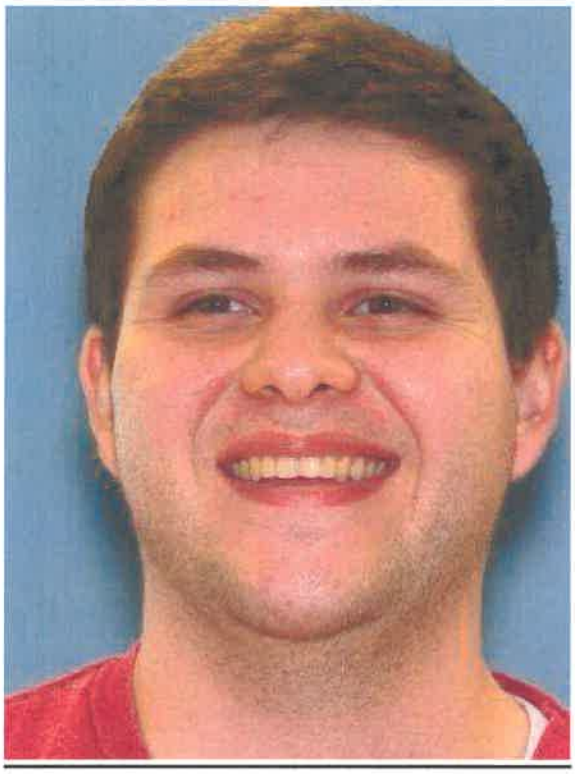
UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

within the SUBJECT PREMISES, such as the private bedroom another resident of the SUBJECT PREMISES, they will not be permitted to search that area.

SUBJECT VEHICLE 1 is a 1998 VOLKSWAGEN JETTA sedan, WA license plate AXE4194.

SUBJECT VEHICLE 2 is a 2003 Volvo sedan, WA plate BMB0759.

The SUBJECT PERSON is KYLE PAUL VANCE (DOB: XX/XX/1995), pictured below:



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT B

ITEMS TO BE SEIZED

The following records, documents, files, or materials, in whatever form, including handmade or mechanical form (such as printed, written, handwritten, or typed), photocopies or other photographic form, and electrical, electronic, and magnetic form (such as CDs, DVDs, smart cards, thumb drives, camera memory cards, electronic notebooks, or any other storage medium), that constitute evidence, instrumentalities, or fruits of violations of 18 U.S.C. § 2422(b) (Enticement of a Minor), 18 U.S.C. § 2251 (Production of Child Pornography), 18 U.S.C. § 2252(a)(2) (Receipt or Distribution of Child Pornography), and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography), which may be found at the SUBJECT PREMISES, in the SUBJECT VEHICLE, or on the SUBJECT PERSON:

1. Any visual depiction of minor(s) engaged in sexually explicit conduct and child erotica, in any format or media and any items depicted in those visual depictions that may help to identify the person depicted or the creator of the depictions;

2. Evidence of the installation and use of P2P software, and any associated logs, saved user names and passwords, shared files, and browsing history;

3. Letters, e-mail, text messages, and other correspondence identifying persons transmitting child pornography, or evidencing the transmission of child pornography, through interstate or foreign commerce, including by mail or by computer;

4. All invoices, purchase agreements, catalogs, canceled checks, money order receipts, credit card statements or other documents pertaining to the transportation or purchasing of images of minors engaged in sexually explicit conduct;

5. Any and all address books, names, lists of names, telephone numbers, and addresses of individuals engaged in the transfer, exchange, or sale of child pornography;

6. Any non-digital recording devices and non-digital media capable of storing images and videos.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

7. Digital devices and/or their components, which include, but are not limited to:

a. Any digital devices and storage device capable of being used to commit, further, or store evidence of the offense listed above;

b. Any digital devices used to facilitate the transmission, creation, display, encoding or storage of data, including word processing equipment, modems, docking stations, monitors, cameras, printers, encryption devices, and optical scanners;

c. Any magnetic, electronic, or optical storage device capable of storing data, such as disks, tapes, CD-ROMs, CD-Rs, CD-RWs, DVDs, printer or memory buffers, smart cards, PC cards, memory sticks, flashdrives, USB/thumb drives, camera memory cards, media cards, electronic notebooks, and personal digital assistants;

d. Any documentation, operating logs and reference manuals regarding the operation of the digital device or software;

e. Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices, or data to be searched;

f. Any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the computer equipment, storage devices or data; and

g. Any passwords, password files, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data;

8. Evidence of who used, owned or controlled any seized digital device(s) at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, saved user names and passwords, documents, and browsing history;

9. Evidence of malware that would allow others to control any seized digital device(s) such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malware; as well as evidence of the lack of such malware;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

10. Evidence of the attachment to the digital device(s) of other storage devices or similar containers for electronic evidence;

11. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from a digital device;

12. Evidence of times the digital device(s) was used;

13. Any other ESI from the digital device(s) necessary to understand how the digital device was used, the purpose of its use, who used it, and when.

14. Records and things evidencing the use of the IP address 73.109.71.123 (the SUBJECT IP ADDRESS) including:

a. Routers, modems, and network equipment used to connect computers to the Internet;

b. Records of Internet Protocol (IP) addresses used;

c. Records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

The seizure of digital devices and/or their components as set forth herein is specifically authorized by this search warrant, not only to the extent that such digital devices constitute instrumentalities of the criminal activity described above, but also for the purpose of the conducting off-site examinations of their contents for evidence, instrumentalities, or fruits of the aforementioned crimes.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970